DHCP Anti-Attack

DHCP Anti-Attack

Normally, when the DHCP client obtains an IP address from the DHCP server, the number of DHCP packets sent by the DHCP client is very small and doesn't affect the performance of the DHCP server. However, a malicious attack can cause the DHCP client to flood DHCP packets to the DHCP server, which will affect the DHCP server performance. To prevent this, you can enable DHCP monitoring on a device.

You can configure a DHCP rate threshold to monitor the packets reaching a device. If the packet rate is equal or higher than the threshold, then the packets are considered as an attack and discarded. The default packets rate threshold is 16pps.

When an attack is detected, the source MAC address of the attack packet is sent to the address table. The address table is maintained with an aging time. When the aging time expires, the table entry with the source MAC address is deleted and packets with the same source MAC address are dropped. The default aging time is 10 minutes. You can modify the aging time. Configure the aging time with a value of 0 prevents the table entry from being deleted.

By default, after an attack all ports are considered as not trustworthy. You can configure a port that does not require monitoring and is trustworthy as a trusted port.

How to Configure DHCP Anti-Attack

Enabling DHCP Packet Monitoring

To enable DHCP packet monitoring, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	[**no**] **dhcp anti-attack** **Example:** `Device(config)# dhcp anti-attack`	Enables DHCP packet monitoring. Use the **no anti-dhcp anti-attack** command to disable DHCP packet monitoring.

Configuring DHCP Rate Threshold

To configure DHCP rate threshold, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	[**no**] **dhcp anti-attack threshold** *value* **Example:** `Device(config)#`	Configures the rate threshold for DHCP packets globally. Use the **no dhcp anti-attack threshold** command to set the default value of 16pps.
Step 4	**interface ethernet** *port-number* **Example:** `Device(config)#`	Enter the port configuration mode.
Step 5	[**no**] **dhcp anti-attack threshold** *value* **Example:** `Device(config-if)#`	(Optional) Configures the rate threshold for DHCP packets on an interface. Use the **no dhcp anti-attack threshold** command to set the default value of 16pps.

Configuring Recovery Function

To configure recovery function, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dhcp anti-attack recover-time** *value* **Example:** `Device(config)#`	(Optional) Configures the recovery time. The default is 10m. Configuring a value of 0 means no aging.
Step 4	**dhcp anti-attack recover** [**all** |*mac-address*] **Example:** `Device(config)#`	Configures the manual recovery. Restores the table items immediately without the need to wait for the aging time to expire.

Configuring Trusted Ports

To configure trusted ports, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface ethernet** *port-number* **Example:** `Device(config)# interface ethernet 0/1`	Enter the port configuration mode.
Step 4	[**no**] **dhcp anti-attack trust** **Example:** `Device(config-ethernet-0/1)# dhcp anti-attack trust`	(Optional) Configures the port as a trusted port. Use the **no dhcp anti-attack trust** command to configure the port as not trusted.

Monitoring DHCP Anti-Attack

The commands in the following table can be used to monitor DHCP anti-attack.

Table 1: Monitoring DHCP Anti-Attack

Command	Purpose
show dhcp anti-attack [**interface ethernet** *port-number*]	Displays the DHCP anti-attack configuration.
show dhcp anti-attack interface ethernet *port-number*	Displays the trusted port configuration.

Example: Anti-DHCP Attack

The following example shows how to configure the anti-DHCP attack.

```
Device> enable
Device# configure terminal
Device(config)# dhcp anti-attack
Device(config)# dhcp anti-attack action deny-dhcp
Device(config)# dhcp anti-attack threshold 1
Device(config)# dhcp anti-attack recover-time 3
Device(config)# logging monitor 0
Device(config)# debug dhcp
Device(config)# show dhcp anti-attack
Dhcp anti-attack: enabled
Dhcp rate limit:1pps
User recovery time:3 minutes
Reject type:DenyDHCP
DeniedSrcMAC       Port     Vlan    DenyType  RemainAgingTime(m)
00:00:00:01:11:23     e1/1     2      DenyDHCP  3

Total entry: 1.

#After 3 minutes, the attack entry is aged out

Device(config)# show dhcp anti-attack
Dhcp anti-attack: enabled
Dhcp rate limit:1pps
User recovery time:3 minutes
Reject type:DenyDHCP
DeniedSrcMAC       Port     Vlan  DenyType  RemainAgingTime(m)

Total entry: 0.
```